Claims

1. A secure transaction system, comprising:

a plurality of information carriers distributed to authorized users for secure storage of information related to carrying out of transactions by said authorized users, each information carrier having a passive data storage medium but lacking any data processing unit, said information stored on said medium being in encrypted form and including transaction messages, crytographic keys, digital signatures and at least one digital certificate issued to an authorized user;

a tamper-resistant drive for reading and writing information relating to transactions on an information carrier presented thereto by an authorized user, said drive connected via a communications link or network to a host computer, said drive having a control unit executing secure protocols for mediating communication between said host computer and drive and between said drive and information carrier, said drive also having a cryptographic processing unit providing encryption and decryption of transaction messages and digital certificates in accord with said secure protocols executed by said control unit and using cryptographic keys, including keys stored by said drive and keys read from said information carriers, as specified by said secure protocols.

2. The system of claim 1 wherein said data processing unit of said drive also providing, as specified by said secure protocols, encryption and decryption of information communicated with said host computer via said communications link.

3. The system of claim 1 wherein said drive includes sensors detecting attempted intrusions into the drive, said control unit being responsive to said sensors for destroying critical cryptographic keys in the drive upon detection of any intrusion.

4. The system of claim 1 wherein said storage medium on said information carrier comprises optical media.

5. The system of claim 4 wherein said information carrier is on optical memory card.

6. The system of claim 4 wherein said information carrier is an optical disk.

7. The system of claim 4 wherein information is stored on said storage medium in accord with a specified format.

8. The system of claim 1 wherein said information stored on said information carrier is in encrypted form corresponding to a decryption key stored in said tamper-resistant drive.

9. The system of claim 8 wherein said information stored on said information carrier also includes personal data for generating keys of said authorized user.

10. The system of claim 9 wherein said personal data comprises any of a personal identification number (PIN), a password, and biometric data.

11. The system of claim 1 wherein said storage medium is logically partitioned and at least one different digital certificate is stored thereon for each partition.

12. The system of claim 1 wherein said secure protocols include an enrollment of an authorized user wherein personal data for said user is digitally signed, and transmitted from a host computer to said drive with at least one digital certificate, and recertified by said drive and stored on said passive storage medium.

13. The system of claim 1 wherein said secure protocols include a transaction by an authorized user wherein transaction requests and authorization information and transmitted between said drive and said host computer and between said drive and said storage medium with at least one digital certificate.

14. The system of claim 1 wherein said secure protocols executed by said drive include at least one protocol that permits modification of said keys stored by said drive.

15. The system of claim 14 wherein said protocol permitting modification of said keys is one of said protocols mediating communications between said host computer and said drive.

16. The system of claim 14 wherein said protocol permitting modification of said keys is one of said protocols mediating communication between said drive and said information carriers.

17. The system of claim 14 wherein at least one of said secure protocols also permits modification of the secure protocols themselves.